

**AFFIDAVIT OF SPECIAL AGENT ADAM M. MORIN
IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

INTRODUCTION

I, Adam Morin, having been first duly sworn, do hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”). I have been employed with the FBI since 2017. I am currently assigned to the Portland, Maine, Resident Office. Prior to joining the FBI, I worked as a Police Officer with the Portland Police Department from 2013 to 2017. Over the course of my law enforcement career, I have investigated a variety of crimes, including drug offenses, sex crimes, firearms offenses, and other offenses related to violent criminal enterprises. I graduated from the State of Maine 25th Basic Law Enforcement Training Program in 2013, and the FBI Basic Field Training Course, 17-03 in 2017. I have attended specialized training related to child sex exploitation.

2. I have probable cause to believe contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A (possession and distribution of child pornography) are located within 42 Sparhawk Street, Apt. 2, Amesbury, Massachusetts (hereinafter the “SUBJECT PREMISES”) and on the person of Daniel STASIAK. I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES and the person of STASIAK, as further described in Attachments A-1 and A-2, respectively, incorporated herein by reference, and to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, as more fully described in Attachments B-1 and B-2, which are also incorporated herein by reference.

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents and other law enforcement officers; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents;

information gathered from the service of administrative subpoenas; the results of physical surveillance conducted by law enforcement agents; and my experience, training, and background as a Special Agent with the FBI. Because this affidavit is submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

BACKGROUND: KIK

4. Kik Messenger is a free messaging application for mobile devices that lets users connect with their friends and the world around them through chat. Users can send text, pictures, videos and more all within the app. Kik uses an existing Wi-Fi connection or data plan to send and receive messages. Kik is available for download through the iOS Apps Store and the Google Play store on most iOS (iPhone/iPod/and iPad) and Android (including Kindle Fire) devices. Kik maintains a distinctive emphasis on privacy and anonymity and was originally targeted towards younger users.

5. Based on my training, experience, review of materials publicly accessible on Kik's website and law enforcement manual, and information provided by other law enforcement officers, I know the following about how Kik works. To register on Kik, a subscriber does not have to register a phone number, only a name and email, with the only constant identification factor being a username that the subscriber selects upon joining. With only a username as an ID, Kik lets the user exchange messages, photos, and videos and other content with others on the platform. Kik users can form private and or public groups whereby a group of individuals with similar interests

may share messages with photos and videos. Public groups are searchable to anybody with the most recent version of Kik and anyone can join as long as there is room within the group.

STATEMENT OF PROBABLE CAUSE

Transfer of Child Pornography via Kik

6. The FBI office in Milwaukee, Wisconsin, in collaboration with the Winnebago County (Wisconsin) Sheriff's Office, conducted a proactive child exploitation investigation targeting nefarious chat groups within the group messaging application Kik. The goal of the investigation was to identify users engaged in the receipt, possession, distribution and possible production of child sexual abuse material.

7. On about April 26, 2020 an online covert employee (OCE) from the Winnebago County Sheriff's Office observed Kik user "danst977" distributing child sexual abuse material within a group on Kik. On April 29, 2020, the user distributed a second video of child sexual abuse. The two videos of child sexual abuse material distributed by the user were captured by the OCE. The video details are listed below:¹

- a. Video 1 depicted a prepubescent male who appeared to be approximately 4 to 6 years old standing in front of an adult female. The adult female performed oral sex on the prepubescent male. This video was sent on 04/26/2020 at approximately 12:23 p.m. CST.

¹ To avoid unnecessary in-person interaction given the health concerns posed by the current pandemic, I am not providing a copy of these videos to the Court. I am aware that the "preferred practice" in the First Circuit is that a magistrate judge view images relied upon for the issuance of a search warrant in this context, to determine whether the images depict the lascivious exhibition of a child's genitals. United States v. Brunette, 256 F.3d 14, 18-19 (1st Cir. 2001). Here, however, the descriptions offered "convey to the magistrate more than [my] mere opinion that the images constitute child pornography." United States v. Burdulis, 753 F. 3d 255, 261 (1st Cir. 2014) (distinguishing Brunette). The children in these paragraphs appear to be no older than six years old – clearly younger than 18 – and the videos depict the children engaged in sexual activity rather than "merely" the lascivious display of the child's genitals. Furthermore, the description of each file is specific as to the child's perceived age and/or physical characteristics. See United States v. Syphers, 426 F.3d 461, 467 (1st Cir. 2005) ("The best practice is for an applicant seeking a warrant based on images of alleged child pornography is for an applicant to append the images *or provide a sufficiently specific description of the images* to enable the magistrate judge to determine independently whether they probably depict real children.") (emphasis added). The description of the files here is sufficiently specific as to the age and appearance of the alleged children and, in both instances, the type of sexual conduct the children are engaged in) that the Court need not view the files to find that they depict child pornography.

- b. Video 2 depicted a nude prepubescent male who appeared to be approximately 4 to 6 years old standing in front of an adult female. The adult female performed oral sex on the prepubescent male. The prepubescent male then urinated into the adult female's mouth. This video was sent on 04/29/2020 at approximately 12:09 p.m. CST.

8. The OCE recorded a video showing user danst977's profile picture and profile information. The profile picture displayed a middle-aged white male with brown eyes and dark colored hair. The profile stated user danst977's name was Dan STASIAK and that the account has been on Kik for 2006 days.

Identification of Kik user "danst977"

9. The FBI served a subpoena to Kik that requested subscriber data for the account associated with username "danst977." The response from Kik included IP logs only from May 10, 2020 to June 8, 2020. Of the 126 reported IP logins, 125 logins originated from IP address 74.65.153.207. Kik provided the following subscriber information:

First Name: Dan
Last Name: Stasiak
Email: danst977@yahoo.com (unconfirmed)²

10. The FBI determined that the internet service provider of the IP address 74.65.153.207 was Charter Communications. The FBI served a subpoena to Charter Communications that requested subscriber information for this IP address for the dates of May 10, 2020, and June 8, 2020 (these dates were the first day and last day an IP login was reported on Kik's IP log). Charter Communications then provided the following subscriber information for the dates of May 10, 2020, and June 8, 2020 as:

Subscriber Name: Doreen Rogan
Subscriber Address: 21 Broadway, York, Maine, 03909

² Kik did not verify the email address provided by the subscriber.

11. I reviewed publicly available Facebook records and determined that Doreen Rogan is Facebook friends with several people with the last name “Stasiak”, although it appears she is not Facebook friends with anyone named “Daniel Stasiak.” At present, I do not know the nature of any relationship between Doreen Rogan and Daniel STASIAK. I have not yet attempted to interview Doreen Rogan out of concern that the covert investigation could be compromised.

12. The FBI served a subpoena to Yahoo Oath Holdings that requested subscriber information and IP logs for email account danst977@yahoo.com. Yahoo provided subscriber information and IP logs from September 8, 2019, to September 8, 2020. Of the 443 reported IP logins, 67 logins originated from IP address 74.65.153.207. The subscriber information for the email account is listed below:

Full Name: dan s
Account Status: Active
City: Ipswich
State: MA
Alternate Email Address: dms92377@hotmail.com (verified)
Phone: +197885196681 (verified)

13. I compared the IP logs produced Kik from the time period of May 10, 2020, to June 8, 2020, and the IP logs produced by Yahoo Oath Holdings from the time period of September 8, 2019, to September 8, 2020 and observed that a user has accessed both the “danst977” Kik account and the danst977@yahoo.com email account from IP address 74.65.153.207.

Identification of the SUBJECT PREMISES

14. Based on my review of open-source databases and vehicle registry information and law enforcement surveillance, I believe that Dan STASIAK has established residency at 42 Sparhawk Street, Apt 2, Amesbury, MA.

15. Open-source research of danst977@yahoo.com, showed that the email was associated to Facebook account “https://www.facebook.com/daniel.stasiak.334.” The Facebook

account display name was “Daniel Stasiak” and it displayed a profile picture that appeared to be the same person as the person displayed on the “danst977” Kik account profile photo. The Facebook account’s timeline noted that STASIAK stopped working at the Sand Dollar Bar & Grill, 2 Beach St, York, Maine, and began working at Brown Sugar by the Sea in Newburyport, Massachusetts, in October 2020.³ The Facebook account’s “check-ins” showed a candy shop in York, Maine, in July 2020, and a restaurant in Amesbury, Massachusetts, in January 2021.⁴ Additionally, the Facebook account revealed that STASIAK likely has two young children, based on publicly available photos.

16. A query of Massachusetts Registry of Motor Vehicle records showed that a person with the name Daniel M. Stasiak and date of birth September 23, 1977, has a suspended driver’s license in Massachusetts.⁵ Furthermore STASIAK’s Massachusetts driver’s license listed his address as 42 Sparhawk Street, Apt 2, Amesbury, MA 01913. The photograph of STASIAK maintained in the Massachusetts Registry of Motor Vehicle records appear to depict the same person as the photographs associated with the “danst977” Kik account and the “Daniel Stasiak” Facebook account and is consistent with the person I observed when I conducted surveillance at 42 Sparhawk Street, Apt 2, Amesbury, MA 01913 on April 20, 2021 (discussed below).

17. A query of the Maine Bureau of Motor Vehicle showed no record for anyone named Daniel Stasiak.

18. Due to STASIAK’s Massachusetts driver’s license listing his address as 42 Sparhawk Street, Apt 2, Amesbury, MA 01913, Facebook activity indicating recent employment

³ A “timeline” is a Facebook specific feature where an account displays a user’s chronological activities to other users.

⁴ A “check-in” is a Facebook feature where a user can virtually announce their location on their timeline.

⁵ Massachusetts Registry of Motor Vehicle records immediately available to law enforcement only display the most recent address for the licensee, it does not display the date that STASIAK’s license was suspended.

in Newburyport, Massachusetts, Facebook activity of “check-ins” in Amesbury, and open-source data indicating that STASIAK resides at 42 Sparhawk Street, Apt 2, Amesbury, MA, the FBI served a second subpoena for subscriber information and IP logs to Yahoo Oath Holdings for email account danst977@yahoo.com seeking updated information. Yahoo Oath Holdings produced an IP log for the time period January 1, 2021, to March 10, 2021. Of the 177 IP logins recorded, 49 logins were IP address 75.67.185.127. Furthermore, Yahoo Oath Holdings produced subscriber information showing no change from subscriber information produced in response to the first subpoena.

19. The FBI served a subpoena to Charter Communications for subscriber information on March 10, 2021, of IP address 75.67.185.127. Charter Communications provided the following subscriber information for March 10, 2021, of IP address 75.67.185.127:

Alissa Johnson
42 Sparhawk Street
Amesbury, MA 01913
617-791-1020
Account Status: Active
Email user ID: alissajohnsonma1@comcast.net

According to a database accessible to law enforcement, Alissa Johnson owns the multi-unit residence located at 42 Sparhawk Street, Amesbury, MA.

20. On April 20, 2021, law enforcement officers conducted surveillance at the SUBJECT PREMISES. At approximately 10:12 a.m., I observed a white juvenile female and a white juvenile male who matched the gender and skin complexion of the children observed on STASIAK’s publicly available Facebook page exit the third-floor side apartment door in the company of a male consistent in appearance with STASIAK. The three walked down the stairs and took a right up the sidewalk. Based upon all of the above, I believe STASIAK currently resides at the SUBJECT PREMISES.

Background on Child Pornography, Computers, and the Internet

21. I have had both training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training and experience, I know the following:

- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
- b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable, or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.
- c. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer, smartphone, or other internet-capable device.
- d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types

– including computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer – can store thousands of images or videos at very high resolution.

It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones are also often carried on an individual’s person.

- e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer, smartphone, or external media in most cases.
- g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with

other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

- h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Characteristics Common to Consumers of Child Pornography

22. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce, advertise, transport, distribute, receive, possess, and/or access with intent to view child pornography (*i.e.*, "consumers" of child pornography):

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including in “hard copy” and electronic format. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Such individuals almost always possess and maintain their hard copies of child pornographic material in the privacy and security of their home or some other secure location. Many individuals who have a sexual interest in children or images of children and who have hard copies of child pornographic material retain that material for many years.
- d. Likewise, such individuals often maintain their digital or electronic child pornography in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor’s residence, inside the possessor’s vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis, sometimes in an attempt to destroy evidence and evade law enforcement. I know through my training and experience that this type of behavior is often seen in individuals who have some level of technical expertise, are aware of law enforcement efforts to investigate child pornography offenses, gain access

to child pornography on anonymized dark web networks like Tor or encrypted mobile applications (which are sometimes perceived by offenders as being “safe” from law enforcement detection), or struggle with their addiction or attraction to child pornography.

- e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals’ computers and other digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.
- f. Such individuals also may correspond with and/or meet others to share information and materials, often retain correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information for individuals with whom they have been in contact and who share the same interests in child pornography.
- g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- h. I submit that even when individuals use a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in their home, including on digital devices other than the portable device (for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices).

23. Based on all of the information contained herein, I believe that STASIAK likely shares characteristics common to consumers of child pornography. In particular, he actively distributed child pornography in an online group chat, indicating a willingness to share and receive child pornography. Given the common characteristics of consumers of child pornography, STASIAK likely has additional child pornography stored at the SUBJECT PREMISES or on his person.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA

24. As described above and in Attachments B-1 and B-2, this application seeks permission to search for records that might be found at the SUBJECT PREMISES or on the person of STASIAK, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in the definition of "computer hardware" in Attachments B-1 and B-2) can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, accessing the internet, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

26. I submit that if a computer or storage medium is found in the place to be searched, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the reasons that follow.

27. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

28. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

29. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

30. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” An internet browser often maintains

a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

31. As further described in Attachments B-1 and B-2, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES or on the person of STASIAK because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish

and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files,

along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

32. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

33. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

34. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

35. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

36. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

- a. The volume of evidence: storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in

random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on site.

- b. Technical requirements: analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.” Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

37. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their

ownership at the premises during the execution of this warrant. If the things described in Attachments B-1 and B-2 are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

38. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachments B-1 and B-2. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

39. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

40. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied, or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents,

attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNLOCKING A DEVICE USING BIOMETRIC FEATURES

41. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.


42. The passcode(s) that would unlock the mobile device(s) belonging to STASIAK are not currently known to law enforcement. Thus, it may be useful to press STASIAK's finger(s) to the devices' fingerprint sensors or to hold the devices up to his face in an attempt to unlock the devices for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

43. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of Daniel STASIAK to the sensor of the devices enabled with biometric unlocking features (or place the device(s) in front of his face, if such feature is enabled) for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

CONCLUSION

44. Based on all of the foregoing, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A, as described in Attachment B-1, are located at the SUBJECT PREMISES, as more fully described in Attachment A-1. I further submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A, as described in Attachment B-2, are located on the person of Daniel STASIAK, as more fully described in Attachments A-2. I respectfully request that this Court issue a search warrant for the locations described in Attachments A-1 and A-2, authorizing the seizure and search of the items described in Attachment B-1 and B-2.

Sworn to under the pains and penalties of perjury,



Special Agent Adam Morin
Federal Bureau of Investigation

SWORN before me telephonically pursuant to Fed. R. Crim. P. 41(d)(3) this 7th day of May, 2021.



HONORABLE JUDITH G. DEIN
UNITED STATES MAGISTRATE JUDGE